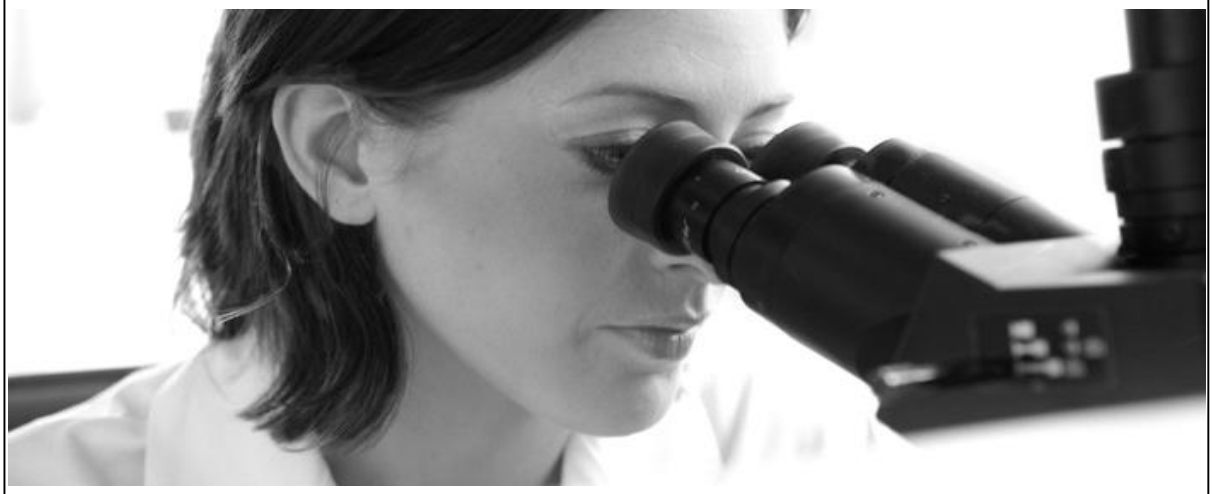
ISSN: 0976-3031

International Journal of Recent Scientific Research

Impact factor: 5.114

ENCRYPTION METHOD USING LSB AND RSA ALGORITHMS IN STEGANOGRAPHY TECHNIQUE



Megha S. Lahase and S. A. Dhole

Volume: 6 Issue: 10

THE PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH
http://www.recentscientific.com
E-mail: recentscientific@gmail.com

Available Online at http://www.recentscientific.com

ISSN: 0976-3031

International Journal of Recent Scientific Research
Vol. 6, Issue, 10, pp. 6695-6698, October, 2015

International Journal of Recent Scientific Research

RESEARCH ARTICLE

ENCRYPTION METHOD USING LSB AND RSA ALGORITHMS IN STEGANOGRAPHY TECHNIQUE

Megha S. Lahase and S. A. Dhole

Department of Electronics and Telecommunication Bharati Vidyapeeth's College of Engineering for Women Pune, India

ARTICLE INFO

Article History:

Received 05th July, 2015
Received in revised form 08th August, 2015
Accepted 10th September, 2015
Published online 28st October, 2015

Key words:

Steganography*; Spartan 3 FPGA; Security; LSB; RSA; Cover image; Secret image.*

ABSTRACT

Steganography is the method that involves communicating secret data in an appropriate multimedia carrier. Many uncommon carrier formats can be used; digital images are the most standard used in steganography. In this paper hybrid combination of least significant bit as well as RSA algorithms are used for encryption process. Inserting secret data inside cover images needs intensive computations, and thus, designing steganography in hardware speeds up steganography. This work indicates a hardware design of Least Significant Bit (LSB) as well as RSA steganography technique in a Papilio Spartan 3 FPGA board.

INTRODUCTION

The term steganography literally means "covered writing" and it is derived from the Greek [1]. It is the branch of cryptography. The dissimilarity between Steganography and Cryptography is that the cryptography attentions on care the matters of a secret message while steganography attentions on care the presence of a secret message. Steganography and cryptography both are ways for keeping data from unwanted parties.

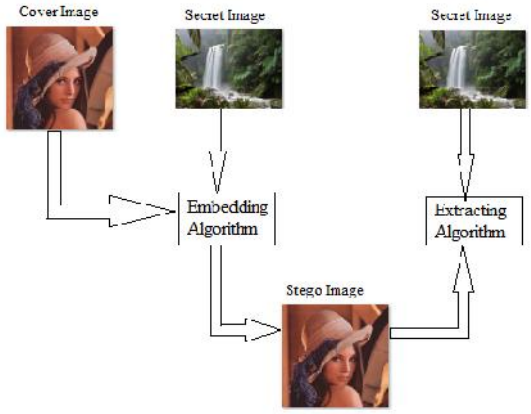


Figure 1 Block diagram of Steganography

Information security of the private information has come to be a dangerous problem in the digital world. Therefore, the demand of having a secure method to transmission the private data is growing.

Generally image steganography is technique of secret image hiding into cover-image and produces a stego-image. This stego-image then sent to another party by recognized medium, wherever the enemy party does not recognize that this stego-image has secreted image. After receiving stego-image hidden image can simply be extracted with or without stego-key by the reception end. Basic block diagram of image steganography is shown in Figure 1 without stego-key, where embedding algorithm needed a cover image with secret image for embedding process. Output of embedding algorithm is a stego-image which mainly sent to extracting algorithm, where extracted algorithms unhide the secret image from stego-image. Steganography is used in images, but several other data or file categories are possible.

1. Audio
2. Video
3. Text
4. Executable programs

Corresponding author:* **Megha S. Lahase
Department of Electronics and Telecommunication Bharati Vidyapeeth's College of Engineering for Women Pune, India

Least Significant Bit (LSB)

There are many types of spatial steganography, all directly replace some bits in the image pixel values in hiding information. LSB-based steganography is one of the simplest methods that hide a secret message in the LSBs of pixel values without observable distortions. To our human eye, changes in the value of the LSB are unnoticeable. LSB replacement method, Matrix inserting are some of the spatial domain methods.

LSB addition is a common and simple method to insert data in an image. The LSB of some or all of the bytes inside an image is altered to a bit of the secret message. Digital images are mostly of two forms (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can insert three bits of data in each pixel, one in each LSB position of the three eight bit values. Growing or reducing the value by altering the LSB does not modification the presence of the image; much so the resultant stego image appearances almost similar as the cover image. In 8 bit images, one bit of data can be concealed.

The LSB of certain or all of the bytes inside an image is changed to a bit of the secret message.

The system has some benefits [1]

- This execution significantly simplifies memory access since it maps one secret byte to one Cover pixel. Reading and handling data at the bytes edge make simpler hardware design and reduces the design area and power.
- The hidden size is third of the cover size, which is considerably improved.

The LSB block receives the three bytes of cover and one byte of the secret, combines them and then provides them back to the AVR8 processor.

The LSB is the lowest significant bit in the byte value of the image pixel [1]. The LSB based image steganography inserts the secret in the LSB of pixel values of the cover image (CVR). To illustrate LSB technique, we gives the following example. Suppose the cover has the following two pixel values:
(0000 1010 0011 0010 0111 0100)
(1111 0101 1100 0011 1100 0111)
Also, assume that the secret bits are: 110110. After embedding the secret bits, the outcome pixel values are:
(0000 101**1** 0011 001**1** 0111 010**0**)
(1111 010**1** 1100 001**1** 1100 011**0**)

The highlighted bits show that the bits were replaced from their original value. Only three bits in the cover image were customized. On average about half of the bits in the cover image will be modified when inserting the secret image.

RSA Algorithm

RSA is a cryptosystem, which is called as one of the first possible public-key cryptosystems and is commonly used for protected data communication. In such a cryptosystem, the encryption key is public and varies from the decryption key which is saved secret. In RSA, this irregularity is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly defined the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent method in 1973, but it wasn't derestricted until 1997.

Simple example of RSA Algorithm

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

FPGA based system for steganography image processing

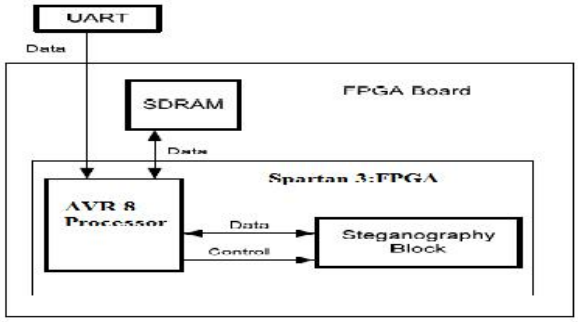


Figure 2 System block diagram

It consists of:

AVR8 Processor
UART Interface
Steganography Unit

The AVR 8-bit microcontroller architecture was introduced in 1997. By 2003, Atmel had shipped 500 million AVR flash microcontrollers. The AVR is a modified Harvard architecture machine where program and data are kept in separate physical memory systems that look in different address spaces, but having the ability to read data items from program memory using special instructions.

A UART (Universal Asynchronous Receiver/Transmitter) is the microchip with programming that controls a computer's interface to its connected serial devices. Specifically, it provides the computer with the RS-232C Data Terminal Equipment.

The steganography block implements LSB steganography method by concealing the secret data in the cover using a combination of 2-bit and 3-bit LSB steganography, referred to as 2/3-LSB [1]. Each CVR pixel is represented by three bytes. A single byte of the secret data is hidden in the three bytes of a cover pixel.

The Papilio One has a Xilinx Spartan 3E FPGA chip, given that a rich quantity of digital logic to quickly get your prototyping

offs the ground. You can code for the FPGA using predictable development tools, or you can take Gadget Factory's custom Arduino IDE to simply write Arduino code and upload it to the AVR8 soft processor.

Encryption Method

By applying an offset to each single byte image Encryption encrypts a secret image into an image [6]. In recent years there have been several reports of secret material such as customers' personal records being uncovered through loss or theft of laptops or backup drives. Encrypting such files at rest helps keep them should physical safety measures fail.

Digital rights management systems, which prevent banned use or duplicate of copyrighted material and protect software against reverse engineering is another somewhat different example of using encryption on information at rest.

Encryption is also used to protect data in transit, for example information being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been many reports of information in transit being intercepted in recent years. Encrypting information in transit also helps to protected it as it is often difficult to physically protect all access to networks.

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar (or different) the stego-image compared with CVR. The following metrics are used in the literature including the work of and:

Mean Squared Error (MSE) is computed by performing byte by byte comparisons of the CVR and stego-image. The computation can be expressed as follows:

$$MSE = \frac{1}{H*W}\sum_{i=1}^{H}\left(P(i,j) \quad S(i,j)\right)^2 \tag{1}$$

Where, H and W are height, width and P (i, j) which represents the cover image and S (i, j) represents its corresponding stego image. Higher value of MSE indicates dissimilarity between cover image as well as stego image.

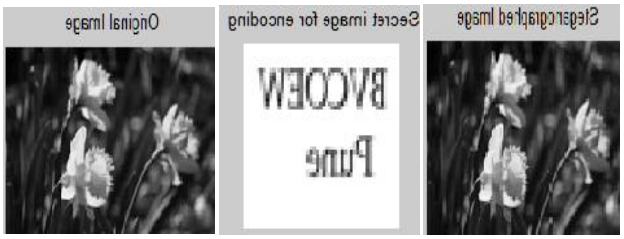
Bit error rate (BER) computes the actual number of bit positions which are changed in the stego-image compared with CVR.

Peak signal-to-noise ratio measures in decibels the quality of the stego-image compared with the CVR. The higher value of PSNR indicates the better quality. PSNR is computed using the following equation:

$$PSNR = 10log_{10}\frac{L^2}{MSE} \tag{2}$$

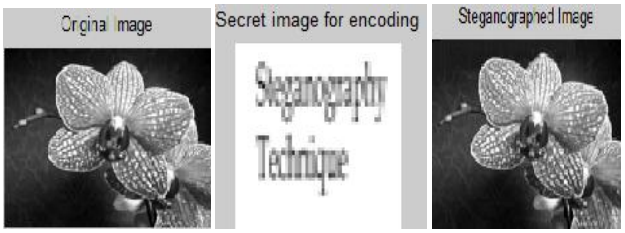
The result stego-images are shown in figure 3. Inspecting the images reveal that the distortion is invisible for the stego-images. The results of the images using LSB algorithm metrics are summarized in Table I and the results using RSA algorithm of the images metrics are summarized in Table II.

EXPERIMENTAL RESULTS IN MATLAB

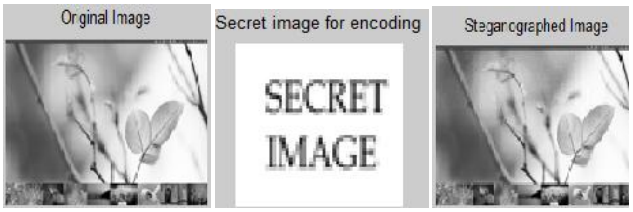


A Steganography between 1 image and 51 image

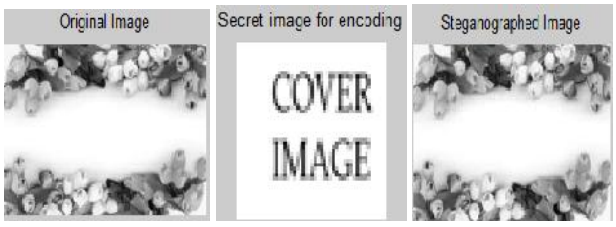
B Steganography between 2 image and 52 image



C Steganography between 3 image and 53 image



D Steganography between 4 image and 54 image



E Steganography between 5 image and 55 image

F Steganography between 6 image and 56 image

Figure 3 Cover images with their Steganographed images

Table I Performance Analysis Using Lsb Algorithm

Cover Images	Secret data	PSNR between Cover image & steganographed image (in dB)	MSE between Cover image & steganographed image	BER between Cover image & steganographed image
1 image.bmp	51 image.jpg	124.1138	0.2545	0.0506
2 image.bmp	52 image.jpg	128.1272	0.1772	0.0503
3 image.bmp	53 image.jpg	123.1267	0.2923	0.0493
4 image.bmp	54 image.jpg	125.2354	0.2367	0.0494
5 image.bmp	55 image.jpg	125.0756	0.2405	0.0482
6 image.bmp	56 image.jpg	109.0999	1.1883	0.0503

Table II Performance Analysis Using Rsa Algorithm

Cover Images	Secret data	PSNR between Cover image & steganographed image (in dB)	MSE between Cover image & steganographed image	BER between Cover image & steganographed image
1 image.bmp	51 image.jpg	121.1411	0.3125	0.0623
2 image.bmp	52 image.jpg	132.8640	0.1104	0.0726
3 image.bmp	53 image.jpg	121.1080	0.3575	0.0588
4 image.bmp	54 image.jpg	125.2354	0.2367	0.0494
5 image.bmp	55 image.jpg	124.6907	0.2499	0.0490
6 image.bmp	56 image.jpg	108.8696	1.2160	0.0511

CONCLUSION

The goal of this paper is to execute two techniques like Steganography and Cryptography for secret communication between the two parties. In our paper we are using an LSB algorithm which represents a high inserting capacity to deliver good image quality & enables simple memory access. In addition to it we are using RSA algorithm for extra security which is based on cryptography. As we are using image as a cover file, high amount of information can be inserted and also provides resistance from enemy. From the table I and II we concluded that PSNR value is better hence the quality of images are better as well as MSE value is less hence the distortion is less.

References

1. B. J. Mohd, S. Abed and T. Al-Hayajneh; "FPGA Hardware of the LSB Steganography Method", *IEEE computers 2014*, pp no.978-1-4673-1550-0/12.
2. C. H. Yanga, C. Y. Wengb, S. J. Wangc, H. M. Sunb;"Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems", Elsevier 2010 pp no. 1635-1643.
3. H. M. Sun, M. E. Wub, M. J. Hinek, C. T. Yang, V. S. Tseng; "Trading decryption for speeding encryption in Rebalanced-RSA"; Elsevier 2009 pp no. 1503-1512
4. Shahzad Alam, Vipin Kumar, W. A Siddiqui and Musheer Ahmad; "Key Dependent Image Steganography Using Edge Detection" 2014 Fourth International Conference on Advanced Computing & Communication Technologies pp no.85-88.
5. Mehdi Hussain and Mureed Hussain; "A Survey of Image Steganography Techniques"; *International Journal of Advanced Science and Technology* Vol. 54, May, 2013 pp no.113-124.
6. Y.Eliza Sruthi, A.Rajaiah, M.Govindu "FPGA Implementation of Lifting DWT Based LSB Steganography"; Reserch article in IJESC, Issue on octomber 2014, pp no.878-884.
7. Anil Kumar, Rohini Sharma; "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique"; *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 7, July 2013 pp no.363- 372
8. Arfan Shaikh, Kirankumar Solanki2, Vishal Uttekar, Neeraj Vishwakarma, "Audio Steganography and Security Using Cryptography", *International Journal of Emerging Technology and Advanced Engineering*, Volume 4, Issue 2, February 2014.
9. Jatin Chaudhari, Dr. K.R.Bhatt, "FPGA Implementation of Image Steganography: A Retrospective"; *International Journal of Engineering Development and Research*; Volume 2, Issue 2, 2014, pp. no.2117-2121.
10. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi; "Image Steganography Techniques: An Overview"; *International Journal of Computer Science and Security*; Volume 6; Issue 3 ;2012; pp no. 168-187.

****

How to cite this article:

Megha S. Lahase and S. A. Dhole. 2015, Encryption Method Using Lsb And Rsa Algorithms In Steganography Technique. *Int J Recent Sci Res.* 6(10), pp. 6695-6698.

International Journal of Recent Scientific Research

ISSN 0976-3031